Security at Vibe

vibe

Overview

With the mission of empowering teams to collaborate, innovate and ideate in a unified canvas, Vibe is a unique all-in-one device with a customized operating system and cloud backed software.
We understand that data security and privacy protection is paramount to our customers. In this paper, we explain what is under the hood of our Vibe system and how it handles user data as well as the measures we adopted to ensure the security and privacy of user data.

Security as company value

At Vibe Inc., we understand that building up trust with our customers is critical to our company's success. Ensuring Data-security and privacy protection are two pillars of trust building. We are continually improving the security, confidentiality, integrity, availability, and privacy of the Vibe system. Our current security policy includes,

- As Vibe Inc. is distributed in a few cities in the US and China, we make sure that all user related data are stored exclusively in US territory.

- Developers in China do not have access to user data. A developer server with mock data is used for development and testing purpose

- Only C-level managers, all of whom have enabled two factor authentication and encrypted their computer, have access to the customer data stored in AWS.

Protecting customer data

Our easy-to-use smartboard software in Vibe is backed by a cloud infrastructure working behind the scenes to ensure near real-time, reliable syncing, sharing and collaboration. Built by experienced system architects with backgrounds from organizations like Twitter and Microsoft on the world's most popular cloud infrastructure, Amazon Web Services (AWS), our system is reliable, scalable, efficient and most importantly, secure.

- ## Data Storage

  The board content is stored in AWS Simple Storage Service (S3). It provides reliable, secure, efficient and scalable storage that millions of applications are already using. The data is further encrypted by the one of the strongest encryption methods, AES-256. As the last line of defense, we do not store board full content into a single image file in S3, but instead break it into a series of stroke, text and images and scattered into the storage. The full image is only composed on the client side.We store users information, teams information and board related metadata into AWS No-SQL database DynamoDB. Users information includes name, email and company information. Teams information includes members, company website, etc. Board metadata includes its creation and last modified time, content URLs to S3 and also access control list. All information is as well encrypted by AES-256.

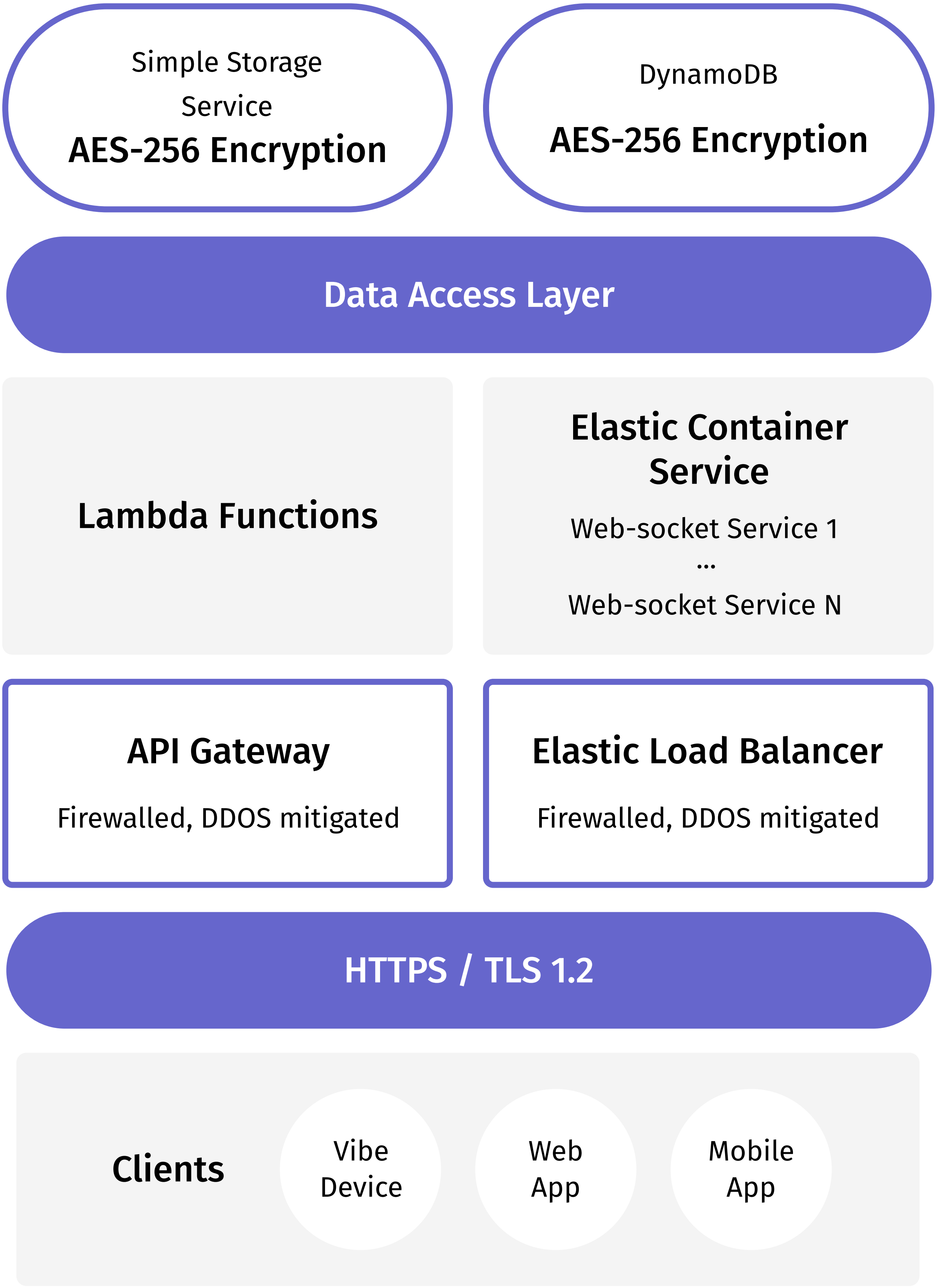
- ## Clients

Vibe clients include the Vibe device, web app and mobile app. All clients communicate with backend systems through HTTPS with TLS 1.2.

Vibe device uses a device unique private key to authenticate with backend system.Web app and mobile app support Single Sign On in additional to password authentication (salted SHA-256 hash).

Once authenticated, backend will issue a JWT token (HS256) for client to authenticate in the future without providing sign in information.

System architecture



Simple Storage Service
AES-256 Encryption

DynamoDB
AES-256 Encryption

Data Access Layer

Lambda Functions

Elastic Container Service
Web-socket Service 1
...
Web-socket Service N

API Gateway
Firewalled, DDOS mitigated

Elastic Load Balancer
Firewalled, DDOS mitigated

HTTPS / TLS 1.2

Clients
Vibe Device
Web App
Mobile App

Talk to an expert?

https://vibe.us

Book a Demo

vibe

Please contact sales@vibe.us for any questions on your specific needs and requirements